REMARKS

This paper is responsive to the Office Action mailed from the Patent and Trademark Office on June 16, 2004, which has a shortened statutory period set to expire September 16, 2004. A petition to revive the application is submitted in a paper filed herewith.

Claims 1-11 are pending in the above-identified application. Claims 1, 2, 5, 6 and 11 are rejected under 35 USC 102, and Claims 3 and 7-10 are rejected under 35 USC 103.

In the current paper, Claims 1, 2, 4, 5, 7 and 10 are amended, and Claims 12-14 are newly entered. No new matter is entered. In view of these amendments and the following remarks, Applicants respectfully request reconsideration and withdrawal of all pending rejections.

Rejections Under 35 USC 102

Claims 1, 2, 5, 6 and 11 are rejected under 35 USC 102(e) as being anticipated by Bjorn (U.S. Patent No. 6,125,192).

Claim 1 is amended herein to recite (in pertinent part) "a non-volatile memory device". Support for this limitation is provided, for example, in original Claim 4, which recites that the memory device is a "flash" memory device. Those skilled in the art recognize that a flash memory device represents one type of non-volatile memory device.

Claim 1 is also amended to incorporate "means for" type claim language that sets forth the functions performed by the processing unit recite in arguably a more appropriate manner. No new matter is entered by this amendment.

Finally, Claim 1 is amended to clarify that the "data retrieving mode … is performed subsequent to the programming mode". Support for this amendment is found, for example, on pages 4 and 5 of Applicant's specification.

No new matter is entered by the above-mentioned amendments.

As amended, Claim 1 recites an electronic data storage medium that is suitable for securely storing personal "data file" information (e.g., a credit card number, a bank account number, or an assigned user identification card number), and for only passing the information to a host system when the electronic data storage medium verifies that the authorized user is present by way of matching a scanned fingerprint with a previously stored fingerprint. The electronic data storage medium therefore includes a "non-volatile [e.g., flash] memory device for storing a data file and fingerprint reference data", both of which being stored during a "programming mode". During a "data retrieving mode" performed subsequent to the "programming mode", "fingerprint scan data" received from a "fingerprint sensor" is compared with the previously-stored fingerprint reference data, thereby allowing the owner of the electronic data storage medium to maintain security control over the stored fingerprint reference data.

In contrast to the electronic data storage medium recited in Applicants' Claim 1, Bjorn teaches a Fingerprint recognition system in which a portion of a scanned fingerprint is transmitted to a host system for preliminary identification (i.e., matching with a fingerprint stored in a database of templates), and then the "preliminary match" is transmitted back to

the "sensor" for "final matching". This process is described with reference to Column 8, line 44 to Column 9, line 12 and Figs. 6A and 6B, which are copied below for reference:

8

At block **625**, a nonce is sent to the sensor **250**. The nonce includes a time/date stamp, the current session key, and other information. It is used to verify the identity of the sensor as well as the currency of the fingerprint.

At block **630**, a differential print is received from the sensor **250**. This, once again, may be an interrupt. The hash is a combination of the nonce, and the differential print, as described above. At block **635**, the hash is decoded, and the nonce is verified. Additionally, the session key may be verified.

At block **640**, the differential print is compared to a database of templates. The database of templates includes all users who are registered with this system. The received print is compared to prints in the database. Such methods are known in the art. Processing continues at block A shown in FIG. **6B**.

Referring to FIG. **6B**, at block **645**, the process of the present invention tests whether a preliminary match was found. If no match was found, the process continues directly to block **670**. If the preliminary match was found, the process continues to block **650**, and both the match and the hash are returned to the sensor for final matching. This is necessary if the digital system, in which actual analysis is done, is not secure. By returning the print and match

9

characteristics to the sensor, the process can be made secure. Alternatively, the final match may be done in the digital system **210**.

At block **655**, a verifying match/no match signal is received from the sensor. Because the sensor is a closed and secure system, the final decision, regarding whether a match was found or not, is left to the sensor. In this way, possible tampering with the digital system **210** does not result in a false positive signal.

At block **660**, it is determined whether the final answer is a yes or a no, i.e. whether the prints match or do not match. If the prints do not match, at block **670**, access is refused.

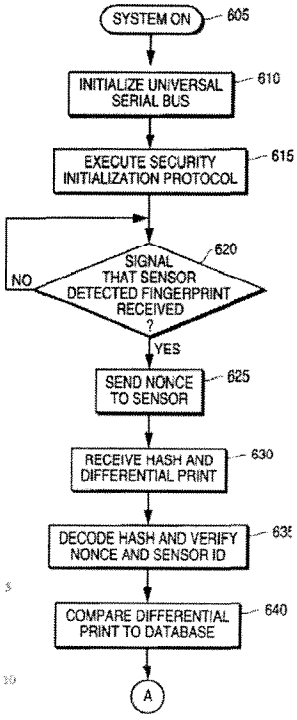

FIG.6A

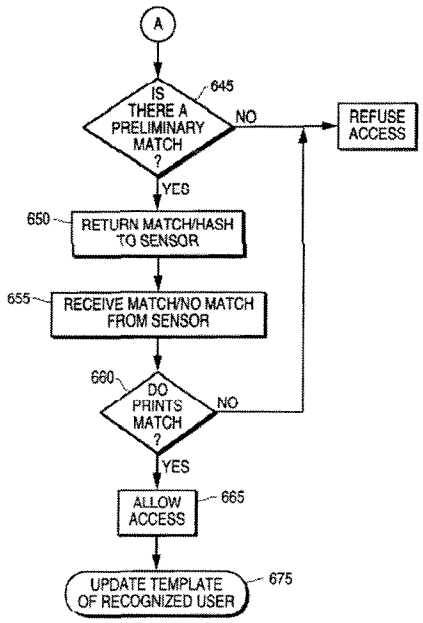

FIG.6B

As recognized by the Examiner in the pending rejection directed to Claim 1 under 35 USC 102, Bjorn fails to teach the storage of fingerprint reference data in a "non-volatile memory device" as recited in Claim 1. Based on the description of Bjorn's system (copied above), Applicant contends that it would not have been obvious to provide either a "non-volatile memory" or "means for controlling said processing using … to store … the fingerprint reference data in said non-volatile memory device" on an electronic data storage medium that includes Bjorn's fingerprint recognition system because the "match" found in Bjorn's step 645 is written from a host

system to the sensor in step 650 during each fingerprint recognition process (see Col. 8, lines 63-65, copied above). That is, because the "match" is written during each fingerprint recognition process, there is no reason to store the "match" for longer than the time it takes to perform the comparison associated with Bjorn's step 660. For this reason, Bjorn in effect teaches away from providing an electronic data storage medium that includes Bjorn's fingerprint recognition system with "non-volatile memory" and "means for controlling said processing unit in a programming mode … to store … the fingerprint reference data in said non-volatile memory device", as recited in Claim 1. Hence, the owner of an electronic data storage medium that includes Bjorn's fingerprint recognition system would not have control over the information stored on the card, thus making the electronic data storage medium unsuitable for, for example, making credit card purchases in stores that do not have access to the "database of templates".

Claims 2, 4, 5, 7 and 10 are amended to be consistent with the amendments entered in Claim 1 (discussed above).

Claims 2, 5, 6 and 11 are dependent from Claim 1, and are therefore distinguished over Bjorn for at least the reasons provided above with reference to Claim 1.

For the above reasons, Applicants' respectfully request reconsideration and withdrawal of the rejections under 35 USC 102.

Rejections Under 35 USC 103

Claims 3 and 7-10 are rejected under 35 USC 103(a) as being unpatentable over Bjorn in view of Jacobsen et al (U.S. Pub. App. No. 2001/0043174).

Claims 3 and 7-10 are dependent from Claim 1, which is distinguished over Bjorn for at least the reasons provided above. Further, Jacobsen fails to overcome the deficiencies of Bjorn that are described above with reference to Claim 1. Hence, it would have been neither possible nor obvious to combine the teachings of Jacobsen and Bjorn to produce the electronic data storage medium recited in Claim 1. Because Claims 3 and 7-10 are dependent from Claim 1, they are believed to be patentable over Bjorn and Jacobsen for at least this reason.

For the above reasons, Applicants' respectfully request reconsideration and withdrawal of the rejections under 35 USC 103.

New Claims

Claims 12-14 are newly entered.

Similar to Claim 1, Claim 12 recites a "non-volatile memory device", a "fingerprint sensor", an "input/output interface circuit", a "processing unit", "means for controlling said processing unit when the electronic data storage medium is in the programming mode" and "means for controlling said processing unit when the electronic data storage medium is in the data retrieving mode". As such, Claim 12 is believed to be distinguished over Bjorn and Jacobsen for reasons similar to those provided above with reference to Claim 1.

In addition, Claim 12 recites "a function key set connected to said processing unit and operably arranged such that a user is enabled to initiate operation of said electronic data storage medium in a selected one of a programming mode and a data retrieving mode by manipulation of the function key set". Support for this amendment is found, for example, on page 5, lines 18-27. The recited "function key" further enhances control of the electronic data storage medium by controlling writing to the non-volatile memory only during the "programming mode". As discussed above, Bjorn's fingerprint recognition system does not involve storing fingerprint reference data in a non-volatile memory of an electronic data storage medium, thus obviating the need for operation in a "programming mode" for this purpose. As such, it would not have been obvious to modify the teachings of Bjorn to include the "function key set" recited in Claim 12.

Claim 13 is dependent from Claim 12, and is therefore distinguished over the cited prior art for reasons similar to those provided above with reference to Claim 12.

Similar to Claim 1, Claim 14 recites a "non-volatile memory device", an "input/output interface circuit", a "processing unit", "means for controlling said processing unit when the electronic data storage medium is in the programming mode" and "means for controlling said processing unit when the electronic data storage medium is in the data retrieving mode". As such, Claim 14 is believed to be distinguished over Bjorn and Jacobsen for reasons similar to those provided above with reference to Claim 1. Claim 14 also recites "means for manually switching the electronic data storage medium between a

programming mode and a data retrieving mode" in a manner similar to that recited above with reference to Claim 12, thus further distinguishing Claim 14 over the teachings of Bjorn and Jacobsen. Note that Claim 14 also recites "security means" that are enabled, for example, by the fingerprint sensor and/or function key set disclosed in Applicant's specification.

CONCLUSION

For the above reasons, Applicants believe Claims 1-14 are believed to be in condition for allowance. Should the Examiner have any questions regarding the present paper, the Examiner is invited to contact the undersigned attorney at the number provided below.

Respectfully submitted,

Reg # 38,186

Patrick T. Bever
Attorney for Applicant
Reg. No. 33,834
408-451-5902

CUSTOMER NO.: 22888